PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
MATTHEW B. DERNIER
KAPLAN & GILMAN, L.L.P.
900 ROUTE 9 NORTH, SUITE 104
WOODBRIDGE, NJ 07095

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing (*day/month/year*)
Applicant's or agent's file reference 436/8/PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US04/10869	International filing date (*day/month/year*) 09 April 2004 (09.04.2004)
Applicant NEW JERSEY INSTITUTE OF TECHNOLOGY	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70.

For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☒ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☒ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Sheikh Ayaz Telephone No. (571) 272-3795

(*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
MATTHEW B. DERNIER
KAPLAN & GILMAN, L.L.P.
900 ROUTE 9 NORTH, SUITE 104
WOODBRIDGE, NJ 07095

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 01 AUG 2006
Applicant's or agent's file reference 436/8/PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US04/10869	International filing date (*day/month/year*) 09 April 2004 (09.04.2004)
Applicant NEW JERSEY INSTITUTE OF TECHNOLOGY	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70.

For more detailed instructions, see the notes on the accompanying sheet.

2. □ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☒ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☒ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

□ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Sheikh Ayaz Telephone No. (571) 272-3795

(*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 436/8/PCT	**FOR FURTHER ACTION** see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/US04/10869	International filing date *(day/month/year)* 09 April 2004 (09.04.2004)	(Earliest) Priority Date *(day/month/year)* 09 April 2003 (09.04.2003)
Applicant NEW JERSEY INSTITUTE OF TECHNOLOGY		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 7 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      □ a translation of the international application into ________________, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. □ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. □ **Certain claims were found unsearchable** (See Box No. II)
3. □ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   □ the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   □ the text is approved as submitted by the applicant.
   ☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☒ as suggested by the applicant.
      □ as selected by this Authority, because the applicant failed to suggest a figure.
      □ as selected by this Authority, because this figure better characterizes the invention.
   b. □ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/10869

Box IV TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

Methods and apparatus for converting original data (106,200) into a plurality of sub-bands (204) using wavelet decomposition (200); encrypting (202) at least one of the sub-bands using a key to produce encrypted sub-band data (208); and transmitting the encrypted sub-band data (208) to a recipient separately from the other sub-bands (104).

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/10869

A. CLASSIFICATION OF SUBJECT MATTER

IPC: **H04L 09/000**
H04L 9/00(2006.01)

USPC: 380/261;713/176

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/261;713/176

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Hotbot(npl)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US6,505,299 B1 (ZENG et al) 07 January 2003 (07.01.2003),entire document	1-3,6-16,19-23
---		-----------
Y		4,5,17,18
Y	SCHNEIER, B., "Applied Cryptography", 2nd edition, John Wiley & Sons, Inc., 1996, pages 584-587	4,5,17,18
A,P	US 2003/0128845 A1 (KUDUMAKIS) 10 July 2003 (10.07.2003), entire document	1-26

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 24 May 2006 (24.05.2006)	Date of mailing of the international search report 01 AUG 2006
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Sheikh Ayaz Telephone No. (571) 272-3795

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
MATTHEW B. DERNIER
KAPLAN & GILMAN, L.L.P.
900 ROUTE 9 NORTH, SUITE 104
WOODBRIDGE, NJ 07095

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*) 01 AUG 2006

Applicant's or agent's file reference 436/8/PCT		**FOR FURTHER ACTION** See paragraph 2 below
International application No. PCT/US04/10869	International filing date (*day/month/year*) 09 April 2004 (09.04.2004)	Priority date (*day/month/year*) 09 April 2003 (09.04.2003)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04L 9/00**(2006.01) H04L 9/00(2006.01)
USPC: 380/261;713/176

Applicant

NEW JERSEY INSTITUTE OF TECHNOLOGY

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
□	Box No. II	Priority
□	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
□	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
□	Box No. VI	Certain documents cited
□	Box No. VII	Certain defects in the international application
☒	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis(b)* that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Date of completion of this opinion 24 May 2006 (24.05.2006)	Authorized officer Sheikh Ayaz Telephone No. (571) 272-3795

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US04/10869

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

□ a translation of the international application into ______, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

□ a sequence listing

□ table(s) related to the sequence listing

b. format of material

□ on paper

□ in electronic form

c. time of filing/furnishing

□ contained in the international application as filed.

□ filed together with the international application in electronic form.

□ furnished subsequently to this Authority for the purposes of search.

3. □ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/10869

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 4-5, 17-18, 24-26	YES
	Claims 1-3,6-16,19-23	NO
Inventive step (IS)	Claims 24-26	YES
	Claims 1-23	NO
Industrial applicability (IA)	Claims 1-26	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US04/10869

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the questions whether the claims are fully supported by the description, are made:

1. Claims 7,20 are objected to under PCT Rule 66.2(a)(v) as lacking clarity under PCT Article 6 because claims 7,20 are indefinite for the following reason(s):
The phrase "a relatively high probability " in claims 7,20 is a relative phrase that renders the claim indefinite. The phrase "a relatively high probability " is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.
As per dependent claims 8-13,21-23, the PCT Rule 66.2(a)(v) objection is inherited by the dependent claims from the independent claims 7,20 and therefore will objected to on the same basis.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/10869

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:

1. DETAILED ACTION

2. Claims 1-26 meet industrial applicability as defined by PCT Article 33(4). The use of multi level security for network data access control is useful in the field of network security/DRM.

4. Claims 1-3, 6-16, 19-23 lack novelty under PCT Article 33(2) as being anticipated by Zeng et al, U.S. Patent No. 6,505,299 B1.

5. As per claim 1; "A method, comprising:
converting original data into
a plurality of sub-bands using
wavelet decomposition [Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the use of '... grouping a set of transform coefficients from a special frequency subband and shuffling the transform coefficients ...', clearly encompasses the claimed limitations, as broadly interpreted by the examiner, insofar as post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing.];
encrypting at least one of the sub-bands using
a key to produce
encrypted sub-band data [Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (key oriented) functions, clearly encompasses the claimed limitations, as broadly interpreted by the examiner.]; and
transmitting the encrypted sub-band data to
a recipient separately from
the other sub-bands [Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the use of cryptographic encryption/decryption (key oriented) functions on post wavelet decomposed sub-band separated data packets, subsequently transferred across the Internet (i.e., a packet oriented, multi-path routed network), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.].".

And further as per claim 14, this claim is an apparatus claim for limitations from the method claim 1 above, and is rejected for the same reasons provided for the claim 23 rejection; "An apparatus including a processor operating under the instructions of a software

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

program, the software program causing the apparatus to perform actions, comprising: converting original data into a plurality of sub-bands using wavelet decomposition; encrypting at least one of the sub-bands using a key to produce encrypted sub-band data; and transmitting the encrypted sub-band data to a recipient separately from the other sub-bands.".

6. Claim 2 ***additionally recites*** the limitations that; "The method of claim 1, further comprising
embedding at least one message in
the at least one sub-band prior to
the encryption step.".
The teachings of Zeng et al (Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (key oriented) functions (insofar as the transform coefficient map is inherently a signature (a digital signature) for the data group/sub-band it is associated with), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 15, this claim is an apparatus claim for limitations from the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection; "The apparatus of claim 14, further comprising embedding at least one message in the at least one sub-band prior to the encryption step.".

7. Claim 3 ***additionally recites*** the limitations that; "The method of claim 2, wherein
the at least one message is at least one of
hashed,
digitally signed for, and
encrypted
prior to embedding the at least one message in
the at least one sub-band.".
The teachings of Zeng et al (Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (key oriented) functions (insofar as the transform coefficient map is inherently a signature (a digital signature) for the data group/sub-band it is associated with), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 16, this claim is an apparatus claim for limitations from the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection; "The apparatus of claim 15, wherein the at least one message is at least one of hashed, digitally signed for, and encrypted prior to embedding the at least one message in the at least one sub-band.".

8. Claim 6 ***additionally recites*** the limitations that; "The method of claim 1, further comprising:
encrypting a plurality of the sub-bands using
respective secret keys to produce
respective encrypted sub-band data,
each secret key being the same or different from
one of more of the respective secret keys; and
transmitting the respective encrypted sub-band data over
at least some differing routes of
a packet-switched network to
the recipient.".
The teachings of Zeng et al (Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (symmetric/secret key oriented) functions, subsequently transferred across the Internet (i.e., a packet oriented, multi-path routed network), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 19, this claim is an apparatus claim for limitations from the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection; "The apparatus of claim 14, further comprising: encrypting a plurality of the sub-bands using respective secret keys to produce respective encrypted sub-band data, each secret key being the same or different from one of more of the respective secret keys; and transmitting the respective encrypted sub-band data over at least some differing routes of a packet-switched network to the recipient.".

9. As per claim 7; "A method, comprising:
permitting a source entity to
make a protocol selection concerning
(i) parameters of a wavelet decomposition process to which
original data are to be subject to
convert the original data into

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

a plurality of sub-bands, and
(ii) parameters of an encryption process to which
at least one of the sub-bands is to be subject to produce
respective encrypted sub-band data; and
permitting the source entity to
select a respective security level to be associated with
the respective encrypted sub-band data;
comparing at least one of
the protocol selection and selected security level(s) with
a database containing data concerning at least one of
(i) a probability that the encrypted sub-band data may be broken
given the protocol selection,
(ii) an association between security levels and protocol selections; and
advising the source entity to
select at least one of a different security level and a different protocol when
a result of the comparison indicates
a relatively high probability that
the encrypted sub-band data may be broken.".

The teachings of Zeng et al (Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (symmetric/secret key oriented) functions, subsequently transferred across the Internet (i.e., a packet oriented, multi-path routed network), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 20, this claim is an apparatus claim for limitations from the method claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection; "An apparatus including a processor operating under the instructions of a software program, the software program causing the apparatus to perform actions, comprising: permitting a source entity to make a protocol selection concerning (i) parameters of a wavelet decomposition process to which original data are to be subject to convert the original data into a plurality of sub-bands, and (ii) parameters of an encryption process to which at least one of the sub-bands is to be subject to produce respective encrypted sub-band data; and permitting the source entity to select a respective security level to be associated with the respective encrypted sub-band data; comparing at least one of the protocol selection and selected security level(s) with a database containing data concerning at least one of (i) a probability that the encrypted sub-band data may be broken given the protocol selection, (ii) an association between security levels and protocol selections; and advising the source entity to select at least one of a different security level and a different protocol when a result of the comparison indicates a relatively high probability that the encrypted sub-band data may be broken.".

10. Claim 8 additionally recites the limitations that; "The method of claim 7, wherein
the protocol selection further includes at least one of:
(i) parameters of a hashing process to which
at least one message is to be subject prior to
embedding the at least one message in
one or more of the sub-bands,
(ii) parameters of a digital signature to which
the at least one message is to be subject prior to
embedding the at least one message in
one or more of the sub-bands,
(iii) parameters of an encryption process to which
the at least one message is to be subject prior to
embedding the at least one message in
one or more of the sub-bands, and
(iv) aspects of nodes of a packet-switched network through which
the respective encrypted sub-band data are to
traverse for transmission to
a recipient.".

The teachings of Zeng et al (Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (symmetric/secret key oriented) functions, subsequently transferred across the Internet (i.e., a packet oriented, multi-path routed network), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 21, this claim is an apparatus claim for limitations from the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection; "The apparatus of claim 20, wherein the protocol selection

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

further includes at least one of: (i) parameters of a hashing process to which at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, (ii) parameters of a digital signature to which the at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, (iii) parameters of an encryption process to which the at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, and (iv) aspects of nodes of a packet-switched network through which the respective encrypted sub-band data are to traverse for transmission to a recipient.".

11. Claim 9 additionally recites the limitations that; "The method of claim 7, further comprising:
converting the original data into
a plurality of sub-bands using
the selected parameters of
the wavelet decomposition process;
encrypting at least one of the sub-bands to produce
encrypted sub-band data using
the selected parameters of the encryption process; and
transmitting the encrypted sub-band data to
the recipient as
one or more separate packets from
the other sub-bands.".

The teachings of Zeng et al (Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (symmetric/secret key oriented) functions, subsequently transferred across the Internet (i.e., a packet oriented, multi-path routed network), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 22, this claim is an apparatus claim for limitations from the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection; "The apparatus of claim 20, further comprising: converting the original data into a plurality of sub-bands using the selected parameters of the wavelet decomposition process; encrypting at least one of the sub-bands to produce encrypted sub-band data using the selected parameters of the encryption process; and transmitting the encrypted sub-band data to the recipient as one or more separate packets from the other sub-bands.".

12. Claim 10 additionally recites the limitations that; "The method of claim 9, further comprising:
encrypting a plurality of the sub-bands using
respective secret keys to produce
respective encrypted sub-band data,
each secret key being the same or different from
one of more of the respective secret keys; and
transmitting the packet(s) of the respective encrypted sub-band data
over at least some differing routes of the packet-switched network to
the recipient.".

The teachings of Zeng et al (Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (symmetric/secret key oriented) functions, subsequently transferred across the Internet (i.e., a packet oriented, multi-path routed network), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 23, this claim is an apparatus claim for limitations from the method claim 10 above, and is rejected for the same reasons provided for the claim 10 rejection; "The apparatus of claim 22, further comprising: encrypting a plurality of the sub-bands using respective secret keys to produce respective encrypted sub-band data, each secret key being the same or different from one of more of the respective secret keys; and transmitting the packet(s) of the respective encrypted sub-band data over at least some differing routes of the packet-switched network to the recipient.".

13. Claim 11 additionally recites the limitations that; "The method of claim 9, further comprising
routing the packet(s) of the encrypted sub-band data to the recipient over trusted nodes of a packet-switched network,
each trusted node having
a node security level for comparison with
the security level(s) associated with
the respective encrypted sub-band data,
wherein each packet may only be routed through
a trusted node having a node security level
equal to or higher than

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

the security level associated with
the encrypted sub-band data.".

The teachings of Zeng et al (Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (symmetric/secret key oriented) functions, subsequently transferred across the Internet (i.e., a packet oriented, multi-path routed network), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

14. Claim 12 additionally recites the limitations that; "The method of claim 11, wherein at least one of:
the node security levels of the trusted nodes are
time variant in response to network conditions; and
each node is capable of
changing its security level in response to the network conditions.".

The teachings of Zeng et al (Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (symmetric/secret key oriented) functions, subsequently transferred across the Internet (i.e., a packet oriented, multi-path routed network), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

15. Claim 13 additionally recites the limitations that; "The method of claim 11, further comprising
merging two or more packets of the respective encrypted sub-band data into
one or more further packets within
a trusted node having a security level equal to or higher than
the security level associated with the encrypted sub-band data.".

The teachings of Zeng et al (Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (symmetric/secret key oriented) functions, subsequently transferred across the Internet (i.e., a packet oriented, multi-path routed network), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

16. Claims 4,5,17,18 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Schneier, B., "Applied Cryptography", 2nd edition, John Wiley & Sons, Inc., 1996, pp 584-587 ('Schneier').

It is noted that Zeng et al, (U.S. Patent No. 6,505,299 B1) does not disclose in the image coding system/method the specific type of encryption used other than to distinguish said encryption as requiring a minimal relatively processing capability. However, it would be obvious to one ordinary skill in the art at the time the invention was made to use generally accepted Schneier disclosed state of the art encryption cryptographic functionality at the time of the invention. Typically this would encompass symmetric key cryptographic functionality (i.e., secret key encryption such as IDEA, etc.,) with accompanying public key cryptographic functionality (i.e., public key encryption such as used in PGP authentication, etc.,).

17. Claim 4 ***additionally recites*** the limitations that; "The method of claim 3, wherein
a private key is employed when
the at least one message is digitally signed for, and
a secret key is employed when
the at least one message is encrypted.".

The teachings of Zeng et al (Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (key oriented) functions (insofar as the transform coefficient map is inherently a signature (a digital signature) for the data group/sub-band it is associated with), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 17, this claim is an apparatus claim for limitations from the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection; "The apparatus of claim 16, wherein a private key is employed when the at least one message is digitally signed for, and a secret key is employed when the at least one message is encrypted.".

18. Claim 5 ***additionally recites*** the limitations that; "The method of claim 1, wherein
the at least one message is
a digital signature,
which is transmitted to
the recipient to
verify the integrity of
the encrypted sub-band data.".

The teachings of Zeng et al (Abstract, col. 1,lines 10-col. 3,line 63, figures 1-17 and associated descriptions, and more particularly

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

figures 11-13,16,17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (key oriented) functions (insofar as the transform coefficient map is inherently a signature (a digital signature) for the data group/sub-band it is associated with), subsequently transferred across the Internet (i.e., a packet oriented, multi-path routed network that encompasses packet authentication at appropriate OSI layers), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 18, this claim is an apparatus claim for limitations from the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection; "The apparatus of claim 14, wherein the at least one message is a digital signature, which is transmitted to the recipient to verify the integrity of the encrypted sub-band data.".

19. Claims 24-26 meet the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest the claim limitations dealing with the wavelet decomposition into encrypted sub-bands independently routed via a packet switched network of trusted nodes associated with security levels used upon successful comparison for access control.

20. As per claim 24; "A system, comprising:
a source entity operable to:
(i) convert original data into
a plurality of sub-bands using
a wavelet decomposition process,
(ii) encrypt at least one of the sub-bands to produce
encrypted sub-band data, and
(iii) transmit one of more packets of the encrypted sub-band data to
a recipient over a packet-switched network separately from
the other sub-bands; and
a plurality of trusted nodes within the packet-switched network,
each trusted node having
a node security level for comparison with
a security level associated with
the encrypted sub-band data,
wherein each packet may only be routed through a trusted node having
a node security level
equal to or higher than
the security level associated with
the encrypted sub-band data.".

21. Claim 25 ***additionally recites*** the limitations that; "The system of claim 24, wherein at least one of:
the node security levels of the trusted nodes are
time variant in response to
network conditions; and
each node is capable of
changing its security level in response to
the network conditions.".

22. Claim 26 ***additionally recites*** the limitations that; "The system of claim 24, wherein at least some of the trusted nodes are operable to
merge two or more packets of the encrypted sub-band data into
one or more further packets
when the given trusted node has
a security level equal to or higher than
the security level associated with
the encrypted sub-band data.".

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under Article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article," "Rule" and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Volume I/A, Annexes B1 and B2).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, Volume I/A, paragraph 296).

What parts of the international application may be amended ?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Preliminary Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When ? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments ?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How ? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments ?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

NOTES TO FORM PCT/ISA/220 (continued)

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

(i) the claim is unchanged;
(ii) the claim is cancelled;
(iii) the claim is new;
(iv) the claim replaces one or more claims as filed;
(v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]: "Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."
2. [Where originally there were 15 claims and after amendment of all claims there are 11]: "Claims 1 to 15 replaced by amended claims 1 to 11."
3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]: "Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or "Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."
4. [Where various kinds of amendments are made]: "Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under Article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments and any accompanying statement, under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the time of filing the amendments (and any statement) with the International Bureau, also file with the International Preliminary Examining Authority a copy of such amendments (and of any statement) and, where required, a translation of such amendments for the procedure before that Authority (see Rules 55.3(a) and 62.2, first sentence). For further information, see the Notes to the demand form (PCT/IPEA/401).

If a demand for international preliminary examination is made, the written opinion of the International Searching Authority will, except in certain cases where the International Preliminary Examining Authority did not act as International Searching Authority and where it has notified the International Bureau under Rule 66.1*bis*(b), be considered to be a written opinion of the International Preliminary Examining Authority. If a demand is made, the applicant may submit to the International Preliminary Examining Authority a reply to the written opinion together, where appropriate, with amendments before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later (Rule 43*bis*.1(c)).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see the *PCT Applicant's Guide*, Volume II.